

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
COLUMBIA DIVISION

In The Matter Of The Search of:) MISC. NO.: 3:24-cr-00167
)
48 Coxsfield Court, Columbia)
South Carolina 29212 (**Target Residence**))
and the person of Malik Bell)

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Stephanie L. McGuigan, a Postal Inspector with the United States Postal Inspection Service ("USPIS"), being duly sworn under oath, depose and state the following:

I. INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant of (1) **TARGET RESIDENCE**, which is the premises at 48 Coxsfield Court, Columbia South Carolina 29212 and any vehicles, outbuildings, or similar structures; and (2) the person of Malik Bell ("BELL"), date of birth May 22, 1997, all for contraband, evidence, fruits, and instrumentalities such as devices and falsified records, identity cards, financial and employment documents, similar things used in the scheme as described below and Attachment B.

2. This affidavit is based upon my personal knowledge, experience, and training, and other information developed during the course of this investigation. This affidavit is also based upon information and experience imparted to me by other law enforcement officers. Because I am submitting this Affidavit for the limited purpose of demonstrating probable cause to search the **TARGET RESIDENCE**, I have not included every fact known about this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that violations of Title 18, United States Code, Section 1708 (Mail Theft) and Title 18, United States Code,

Section 1344 (Bank Fraud) have been committed and that the TARGET RESIDENCE and person of Malik Bell contain evidence, fruits, and instrumentalities of this violation and contraband, as further described in Attachment B of this Affidavit.

3. I am a United States Postal Inspector and have been so employed for over seven years, presently assigned in Columbia, South Carolina to investigate crimes involving the United States Mail, including mail theft, mail fraud and financial crimes that utilize the United States Postal Service ("USPS"). As a United States Postal Inspector, I have experience and received training in the investigation of the theft of United States Mail, as well as crimes of fraud committed with stolen mail. I was previously a Border Patrol Agent with the United States Border Patrol where I served for five years.

4. As it relates to the requested search, based on my training and experience, and participation in mail theft and bank fraud investigations I know:

- a. Such fraud schemes are commonly organized using and facilitated by electronic devices such as cellular telephones and laptop/desktop computer. Co-conspirators commonly used such devices to engage in schemes such as the ones described in this affidavit that are coordinated and organized by multiple co-conspirators. This is shown in this particular investigation where the target described below commonly uses the electronic equipment as do all other conspirators to facilitate this scheme.
- b. Conspirators also often maintain and access discrete or hidden locations while using stolen identities to further the scheme and to avoid detection by law enforcement. Such information is evidence of criminal conduct and contraband, so they are commonly protected in secure locations, such as residences or stash locations, safes, closets, or storage units. Devices such as the one sought to be searched here often help agents identify such locations, which provides relevant and probative evidence.
- c. That persons involved in mail theft and bank fraud conceal in secure locations, with ease of access, large amounts of currency and other proceeds of mail theft

and bank fraud and evidence related to obtaining, transferring, secreting, and spending of fraud transaction proceeds.

- d. That it is common for the persons involved in mail theft and bank fraud to keep and maintain records and other evidence of mail theft and bank fraud conduct at such locations.
- e. Finally, I know based on my training and experience that persons involved in schemes such as those described herein may seek to place or launder fraud proceeds into cryptocurrency assets. Such conduct allows targets a perceived ability to conceal and maintain fruits and proceeds of the fraud scheme. The use of the Dark Web is evidence of a target's sophisticated ability to use the internet and such means to facilitate fraud scheme.

II. TARGET OFFENSES

5. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that co-conspirators in this case and Malik Bell have committed violations of Title 18, United States Code, Sections 1708 (Mail Theft) and 1344 (Bank Fraud). I further submit there is probable cause to believe that if the requested searches are approved, agents would recover relevant and probative evidence, instrumentalities, and contraband of these crimes, as set forth in Attachment B.

III. BACKGROUND AND SUMMARY OF STATE INVESTIGATION

6. As explained in further detail below, I believe Malik BELL has been engaged in an ongoing mail theft and bank fraud scheme. BELL and other co-conspirators steal mail from large depositories, typically outside post offices. The conspirators then use chemical agents to remove the payee and amount information from the checks, commonly called "check washing." The co-conspirators then either sell the blank checks for profit using social media or alter to check and attempt to deposit forged and fraudulent amounts in co-conspirator bank accounts. State law enforcement has identified other co-conspirators and served previous search warrants. Those

search warrants have uncovered evidence that BELL is involved in the scheme and that additional evidence of mail theft and bank fraud will be located on his person and at the TARGET RESIDENCE.

7. On June 22, 2023, the South Carolina Enforcement Division (SLED) began investigating a widespread fraudulent check ring in South Carolina as reported by the Ehrhardt Police Department, Bamberg County Sheriff's Office, Allendale Police Department, Hampton Police Department, Hardeeville Police Department, Beaufort County Sheriff's Office Aiken County Sheriff's Office, and the Estill Police Department. All the above agencies identified individuals that had been recent victims of forgery and check fraud. The victims reported they mailed checks through U.S. Postal Service but the checks never reached their destination. Shortly after mailing the checks, they were informed by their respective banks that their checks had been counterfeited and/or reproduced and made payable to other, unauthorized persons. Most of the checks were mobile deposited through online banking, while others were believed to have been deposited through ATM machines. Investigation determined the funds were then withdrawn from ATM machines.

8. During the investigation, Agents located and identified an individual who had a counterfeit check payable to them. The individual was willing to cooperate with the investigation and became Cooperating Defendant #1 (CD #1). CD #1 told Agents that they observed a social media post soliciting individuals to "tap in". The investigation has determined the term "tap in" is commonly used on social media platforms, including Facebook, Instagram, Snapchat, and Telegram by individuals involved in mail theft and check forgery to solicit bank account information from potential co-conspirators. CD #1 reported that the social media posts had a list of banks including but not limited to; South State Bank, SRP Federal Credit Union, Bank of America, Navy Federal

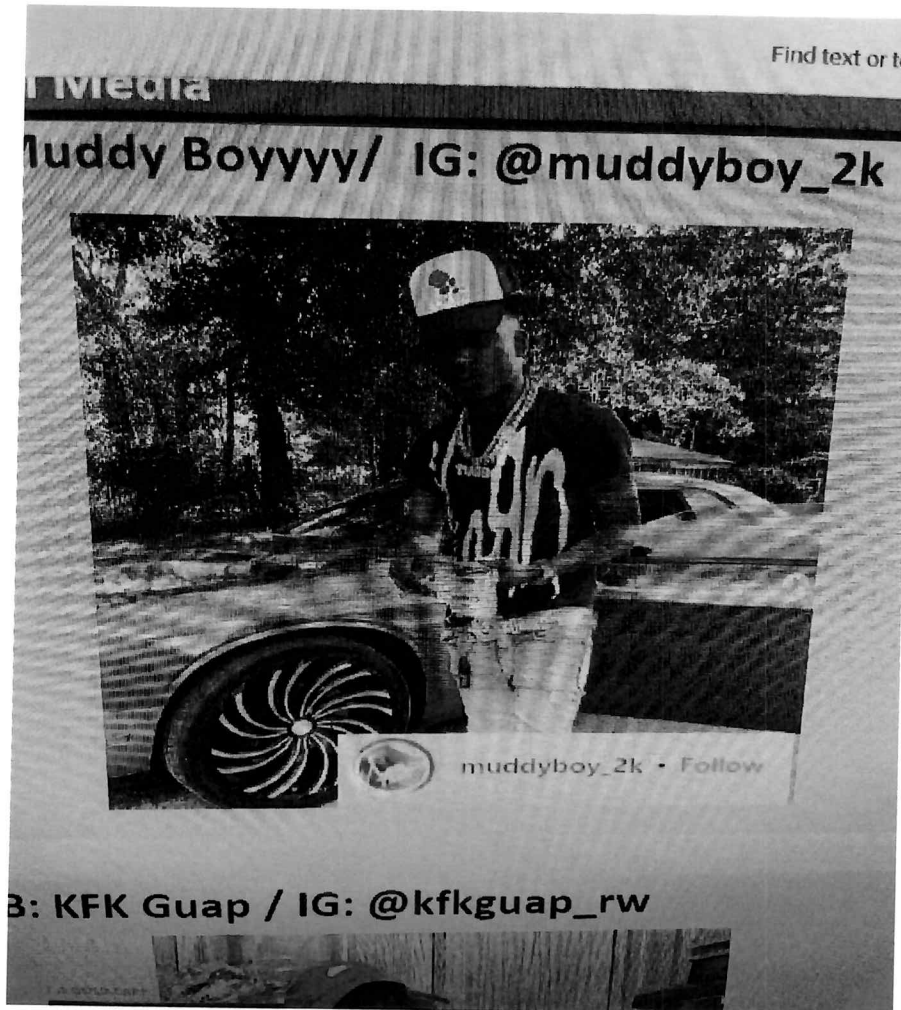
Credit Union, and Truist Bank. CD #1 contacted the individual who made the post. The subject who made the post, Tyquavien JOYNER, requested CD #1 provide him with their mobile bank login, as well as their debit card. CD #1 willingly provided JOYNER with their Wells Fargo banking information via telephone calls and Facebook Messenger messages. CD #1 was told they would receive a portion of the proceeds obtained through the negotiation of any fraudulent checks deposited to their account. CD #1 said they did not know where the checks came from.

9. On June 20, 2023, a fraudulent check from Ag Spray Company/Michael Mathias in the amount \$3,200.00 was deposited into CD #1's bank account. Several attempts were made by JOYNER to withdraw the funds on the mobile banking app using CD #1's log in information. JOYNER logged into CD #1's banking app repeatedly. The bank of deposit identified the transaction as fraud and the transaction was cancelled.

10. CD #1 informed Agents that several other individuals from the Hampton and Allendale area were making social media posts on Facebook and Instagram to recruit other users to "tap in". CD #1 provided Agents with the usernames and actual names of the individuals. Agents conducted surveillance of each of their profiles and observed multiple posts asking users to "tap in".

11. The Facebook Username of "Muddy Boyyy" was identified as one of the suspects recruiting users for the fraudulent scam. The same subject is also utilizing the Instagram username of @muddyboy _ 2K. This subject was positively identified as D'angelo GADSON. CD #1 informed Agents that GADSON and other co-conspirators were staying at an unknown location in the Columbia area. CD #1 stated that GADSON had printers capable of printing counterfeit checks at the residence in Columbia. Gadson also allegedly had in his residence materials used to remove ink from stolen checks so they could be counterfeited; a process known as check washing.

12. Through investigation, GADSON was located, and a state search warrant was conducted at his residence, 164 Beckett Lane Columbia, SC 29223. Agent's reviewed GADSON's social media accounts and observed him posing for photographs in front of a green Dodge Challenger with black and silver rims. In photos, GADSON is seen holding large amounts of US currency standing in front of the vehicle.



13. On August 7, 2023, Palmetto State Bank notified Agents of another victim. The victim was identified as Brunson Building Supply in Hampton County, SC. A check that had been written by Brunson Building Supply was stolen, counterfeited, and presented to a Navy Federal Credit Union in the Savannah, Georgia area. The altered and forged check was made payable to Alphonzo

MOTON, also of Hampton, SC. Agents conducted an interview of the Brunson Building Supply employee who wrote the check. The employee advised she placed the check along with several other checks into the blue mailbox outside the Hampton Post Office. The employee advised that she put the check into the mailbox, along with several other checks on August 1, 2023, between 5:30pm and 6:00pm.

14. On August 10, 2023, Agents went to the Hampton, SC Post office located at 604 151 Street W Hampton, SC, 29924 to conduct an inspection of the blue collection box. There was no signs of forced entry and no other reports of anyone attempting or breaking into the blue collection box.

15. Agents located surveillance footage in the area. The employee of Brunson Building Supply was observed approaching the mailbox on August 1, 2023, at 5:55pm. On August 2, 2023, at 12:27 a.m., a vehicle was seen pulling up to the mailbox. A subject was seen exiting the vehicle. The vehicle then left the area of the mailbox and drove around the block. Approximately ten minutes later, the vehicle returned and once again pulled up to the mailbox. This is consistent with the mail theft technique known as “fishing,” where an individual will stick a flexible object into the mail receptacle with a sticky substance to “fish” mail out of a collection box. Subjects often use this technique because it does not damage the collection box or alert the postal service that the box has been breached. Subjects that are attempting to “fish” mail out of mail receptacles will do so in the middle of the night, after the post office has closed, and there is a not lot of traffic. Legitimate USPS customers who are conducting mail drop off at a USPS collection box usually only park in front of the collection box long enough to drop their mail into the receptacle and drive away. They have no need to exit the vehicle. The vehicle then left the area by driving through the parking lot of the Hampton County Fire Department. The vehicle made a left onto Walnut Street directly in

front of the Hampton County EMS building. Although the video is grainy, the vehicle appears consistent with GADSON's green Dodge Challenger.



16. Agents conducted a visual description search for the Green Challenger through license plate reader databases. Agents were able to positively identify the vehicle as the one GADSON was pictured with from License plate reader databases based on location of the LPR hits, unique stickers, rims, and the color of the vehicle with a black stripe. Image from LPR Flock reader below:



17. On August 16, 2023, law enforcement conducted a search warrant of GADSON's residence at 164 Beckett Lane Columbia, SC 29223. Agents found and seized the Brunson Building Supply envelope that was stolen from the Hampton Post Office. The search also resulted in the discovery of items used to make counterfeit checks such as blank check stock paper, printer ink, and multiple debit cards in different people's names from different banks as well as multiple banks documents from different individuals, and blank check stock paper. Law enforcement also found ATM deposit slips, several magnetic credit card chip readers, and several binders containing car titles and notes in the home.

18. Further, law enforcement discovered a black and brown belt covered in a sticky substance in the residence. This is consistent with the mail theft technique known as "fishing," where an individual will stick a flexible object into the mail receptacle with a sticky substance to "fish" mail out of a collection box. Subjects often use this technique because it does not damage the collection box or alert the postal service that the box has been breached.

IV. PROBABLE CAUSE

19. GADSON was located at the residence and arrested at the time of the state search. He was transported to the Hampton County Detention Center. During the transport, GADSON told agents "Ya'll have the wrong guy." He stated that "Leek Obama" was the leader of the fraud ring.

20. On August 17, 2023, the SLED Fusion Center completed an intelligence packet on the alias "Leek Obama". The SLED Fusion Center was able to identify the subject as Malik BELL, of Orangeburg, SC. A social media review was completed of BELL's social media accounts. BELL is a musician that uses the stage name, "Leek Obama." Agents discovered a Facebook profile picture with BELL's picture using the "Leek Obama" name.



21. BELL made several posts on Facebook and Instagram attempting to recruit other users to "tap in" and was promising them various amounts of financial gain in return. BELL's posts were very similar to posts made by GADSON and other suspects involved in this case. BELL posted photographs of himself holding large amounts of US currency.



22. Another individual identified by CD #1 was Kevin DUNBAR Jr., aka "Go Insta Kev". Since June 2023, agents have conducted ongoing surveillance of DUNBAR's Facebook account. On or about January 3, 2024, DUNBAR posted "Bank of America, Navy, Truist/BB&T need one of these ASAP! Wells Fargo." On or about January 2, 2024, DUNBAR posted "First round. Swing all account 3 months or better w good history (debit card emoji)." On or about December 18, 2023, DUNBAR posted "BofA, Truist/BB&T, Navy Fed, Chase, Get n da Looop (Cash emoji)." Those Facebook posts have since been deleted. Investigation has revealed these posts are used to solicit collusive account holders to provide their banking information and access to financial accounts to launder proceeds of counterfeit checks.

23. During the week of January 29, 2024, SLED agents identified DUNBAR's primary residence as 909 Holly Street West Columbia, SC. On February 1, 2024, arrest warrants for DUNBAR and a state search warrant were executed at 909 Holly Street, West Hampton, SC for Forgery and Crimes Against a Federally Chartered Institution. After being informed of his rights and signing a *Miranda* waiver, DUNBAR agreed to answer questions. Agents interviewed DUNBAR.

24. DUNBAR stated he has been participating in the "tap in" check fraud scam for approximately one year. He indicated Malik BELL trained him on how to carry out the scam. DUNBAR said he had cashed approximately 100 checks in the past year and had personally profited approximately \$7,000. He had initially been purchasing washed checks from BELL for \$100, however, BELL had trained him on how to utilize the website "ocw.com"¹ to facilitate the scam. Over the past year, DUNBAR recruited approximately 75 people to "tap in" to the scam.

25. DUNBAR stated BELL has several individuals working for him, and BELL had "a lot of cash." DUNBAR stated he had just been to BELL's "Coxfield" house in Irmo, SC where he observed several debit cards in plain view, that he believed were linked to financial crimes. The "Coxfield" house he is referring to is Malik BELL's residence of 48 Coxsfield Court Columbia SC 29212. IP address records show DUNBAR at 48 Coxsfield Court Columbia, SC 29212 on January 30, 2024.

26. According to records from the South Carolina Department of Employee Workforce (SC DEW), BELL has not had a job that reports wages in several years. 48 Coxsfield Court is the address listed on BELL's driver's license, and the only vehicle registered to BELL is a Dodge Charger with an associated address of 48 Coxsfield Court. It appears that Coxfield Court is BELL's residence and that it is likely that the address contains evidence of BELL's connections to the mail theft and bank fraud scheme.

27. As part of the investigation, Agents obtained subpoenas for cell phone subscriber and cell records for known cell phone numbers for GADSON and DUNBAR, as well a court order for cell phone tower information, also known as a "tower dump", for any cell phone activity on cell phone towers near the crime scene at or around the time the fraudulent activity occurred. The information

¹ ocw.com provides online check writing services.

contained on GADSON and DUNBAR's cell phones contained Facebook and SMS text messages with BELL communicating about the fraudulent scheme and photographs of stolen or counterfeit checks.

28. To date, agents have identified at least 100 checks that are believed to have been stolen from the mail before being washed, counterfeited and/or reproduced. The counterfeit checks were then presented for deposit at multiple federally chartered institutions in South Carolina, Georgia, and other unknown locations. The total value of the checks believed to be connected to victims across the Allendale, Hampton, and Beaufort areas is at least \$180,000.

29. On December 31, 2023, BELL was pulled over by Richland County Sheriff's Department while driving a black Dodge Charger bearing an expired SC paper tag. BELL was driving two passengers. BELL's driver's license was suspended. After a probable cause search, a backpack with approximately \$50,000 cash, plastic bags with green plant like material, a Zastava 7.62 AK 47 Pistol, and a black Glock and a tan Glock handgun were found. BELL and his two passengers were arrested for PWID marijuana, and a juvenile was charged with the possession of the firearms.

30. Currently, BELL has an outstanding warrant from Augusta, GA (2020) for failure to appear.

V. NEXUS OF ITEMS TO TARGET RESIDENCE

31. Based on my training and experience from investigating numerous mail theft cases, I know that individuals involved in bank and mail schemes retain possession of stolen mail. Evidence of stolen mail often includes open envelopes and pieces of mail including letters, cards, and mailers addressed to multiple individuals. Additionally, based on my training and experience from investigating mail theft and bank fraud cases, I know that individuals involved in these schemes often retain documentary evidence in the form of checks, debit and credit cards, bank statements,

and false, fraudulent, and unlawful identification information. Additionally, individuals involved in this type of scheme also typically possess electronic devices capable of creating false and fraudulent checks, debit and credit cards including computers, cell phones, tablets, printers, magnetic encoders, and other hardware.

32. Further, individuals suspected of involvement in this particular mail and bank scheme have been found to have:

- a. USPS Mail addressed to other individuals
- b. Cellular phones
- c. Blank check stock paper
- d. Debit/credit/bank cards from various financial institutions
- e. Printer ink cartridges
- f. Magnetic card readers
- g. Checks payable to other individuals
- h. Notebooks/ledgers
- i. Tablets
- j. ATM receipts
- k. Check receipts
- l. Financial institutions deposit and withdrawal receipts
- m. Belts covered in an adhesive substance

33. During this investigation, as described previously, search warrants were conducted at both GADSON and DUNBAR's residences. GADSON was in possession of two cell phones at the time of the search and agents seized an additional eight cell phones from the residence. DUNBAR was in possession of one phone however he stated that the phone has only been in use for 30 days.

Ongoing surveillance of social media accounts show that the subjects involved in this fraudulent scheme are using multiple phones, laptops, and tablets to access banking information and communicate with each other. BELL has posted Facebook stories showing videos of himself recording other laptops and phones. DUNBAR's phone contained messages via Facebook Messenger to and from Malik BELL. I believe based on the activity of the subjects involved in this case it would be a reasonable conclusion that BELL and other subjects would be in possession of multiple cell phones and electronic devices that would contain evidence of Mail Fraud, Bank Fraud, and Wire Fraud.

34. Based on my training and experience from investigating numerous mail theft cases, I know that individuals in possession of tools to compromise USPS mail receptacles (such as homemade "fishing" devices) will often travel to different locations by vehicle and attempt to use these items to steal mail from mail collection boxes. In my experience, mail thieves and people who are stealing and creating counterfeit checks often leave or store these items in their vehicle if they do not return them to their residence. Therefore, it is a reasonable inference that tools of mail theft and stolen checks may also be kept in their vehicle so that the fishing tools would be readily available to commit thefts from mail receptacles.

VI. CELL PHONES AND CELL PHONE DATA

35. Based on my training and experience, I know that "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018) (citing *Riley v. California*, 573 U.S. 373, 385 (2014)). Based on my training and experience, I know that it is common for the subjects of federal investigations to carry cell phones during the commission of criminal conduct, a substantial number of which are smart phones that have access to many

different texting applications, or apps, that allow users to communicate with one another that would not be seen or apparent upon the examination of cell phone records from cell phone providers.

36. Based on my knowledge, training, and experience, I also know that electronic devices such as cell phones can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on such devices. This information can sometimes be recovered with forensics tools.

37. There is probable cause to believe that things that were once stored on cell phones may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

38. This warrant seeks permission to seize any cellular phones and other electronic devices, described in Attachment B, that are located within the TARGET RESIDENCE, as described in Attachment A. If and when these cellular phones are located and seized, a separate search warrant will be sought and applied for to request permission to conduct a forensic analysis on said phone(s), where they can be more specifically described and identified.

CONCLUSION

39. Based on the foregoing information provided in this affidavit, I feel that there is probable cause to believe that evidence, fruits, and instrumentalities, further described in Attachment B of this Affidavit, in violation of Title 18 United States Code, Section 1708 (Mail Theft) and Title 18 United States Code 1344 (Bank Fraud), exists within the TARGET RESIDENCE belonging to BELL and others involved in committing fraudulent activity, further described in Attachment A of this Affidavit.

40. I further request, by way of a separate motion and proposed Order to Seal and for the reasons stated in that motion, that the Court order that all documents related to this application, including the affidavit and search warrant, be sealed until further order of the Court or from one year from the date of the sealing Order.

This affidavit has been reviewed by Assistant United States Attorney DeWayne Pearson.


I swear, under penalty of perjury, that the foregoing is true and correct to the best of my knowledge.


Stephanie L. McGuigan
U.S. Postal Inspector

SWORN TO ME VIA TELEPHONE OR
OTHER RELIABLE ELECTRONIC MEANS
AND SIGNED BY ME PURSUANT TO
FED. R. CRIM. P. 4.1 AND 4(d) OR 41(d)(3),
AS APPLICABLE.

This 14th day of Feb. 2024
Columbia, South Carolina

This affidavit was sworn to by the affiant, who attested to its contents pursuant to Fed. R. Crim. P. 4.1(b)(2)(A) by telephone after a document was transmitted by email pursuant to Fed. R. Crim. P. 4.1.


Honorable Shiva V. Hodges
United States Magistrate Judge

